

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

*

PAMELA CHAMBLISS, *et al.*,

*

Plaintiffs,

*

v.

Civil Action No. RDB-15-2288

*

CAREFIRST, INC, *et al.*,

*

Defendants.

* * * * *

MEMORANDUM OPINION

Plaintiffs Pamela Chambliss (“Chambliss”) and Scott Adamson (“Adamson”) (collectively, “Plaintiffs”) bring this putative class action against Defendants CareFirst, Inc., CareFirst of Maryland, Inc. (collectively, “Defendants” or “CareFirst”),¹ and Does 1-10,² alleging various tort, negligence, and statutory claims arising under Maryland law. Specifically, Plaintiffs claim that Defendants failed to secure adequately the computer hardware storing their customers’ personal information, including names, birth dates, email addresses, and subscriber identification numbers.

Presently pending is Defendants’ Motion to Dismiss (ECF No. 11). This Court held a hearing on the pending Motion on May 19, 2016. For the reasons that follow, Defendants’ Motion to Dismiss (ECF No. 11) is GRANTED. In sum, Plaintiffs have failed to allege facts

¹ CareFirst, Inc. and CareFirst of Maryland, Inc. are entities incorporated under Maryland law with their respective headquarters also in Maryland. Compl. ¶¶ 4-5, ECF No. 1. CareFirst of Maryland, Inc. is allegedly a unit or subsidiary of CareFirst, Inc., however Plaintiffs’ substantive allegations do not distinguish between the two Defendants. *Id.* Although Plaintiffs name CareFirst, Inc. and CareFirst of Maryland, Inc. as separate defendants, this Court will also refer to Defendants collectively as “CareFirst.”

² Plaintiffs allege that Does 1-10 are legally responsible for the events underlying this action, and thus proximately caused Plaintiffs’ alleged damages. Compl. ¶ 6. As Plaintiffs do not have standing under Article III of the Constitution, any claims against Does 1-10 are also dismissed.

sufficient to establish standing under Article III of the Constitution. Accordingly, this Court does not have subject matter jurisdiction to adjudicate their claims. All claims are thus DISMISSED.

BACKGROUND

At the motion to dismiss stage, this Court accepts as true the facts alleged in the plaintiff's complaint. *See Aziz v. Alcolac, Inc.*, 658 F.3d 388, 390 (4th Cir. 2011). This case arises out of a well-publicized data breach at Defendant CareFirst, a health insurance provider operating in Maryland, Virginia, and the District of Columbia. Compl. ¶ 10, ECF No. 1. On May 20, 2015, CareFirst announced that it had discovered a data breach that allegedly compromised the confidential personal information of approximately 1.1 million individuals. *Id.* ¶ 12. Two data breaches allegedly occurred: the first in June 2014, and the second immediately prior to CareFirst's announcement on May 20, 2015. *Id.* ¶¶ 14-15. This personal information included the names, birth dates, email addresses, and subscriber identification numbers of the affected individuals. *Id.* ¶ 1. CareFirst denied that any confidential medical records were implicated in the breach. *Id.* ¶ 1 n.1.

At the time of the breach, named Plaintiffs Pamela Chambliss and Scott Adamson held health insurance issued by CareFirst.³ *Id.* ¶ 11. They seek to bring a putative class action on behalf of other holders of CareFirst health insurance. *Id.* Plaintiffs allege that CareFirst knew or should have known earlier of both breaches, as the information stolen is allegedly "highly coveted by and a frequent target of hackers." *Id.* ¶¶ 14, 17. Plaintiffs claim that the potential ramifications of the theft of this data are substantial. *Id.* ¶¶ 16-19. As customers of

³ Chambliss is no longer insured by CareFirst, however Adamson remains a CareFirst customer at this time. *Id.* ¶¶ 22-23.

CareFirst, Plaintiffs allege that they had a reasonable expectation that their confidential personal information would remain private and confidential. *Id.* ¶ 21. Due to CareFirst's failure to secure the personal information at issue, Plaintiffs claim that they and the class members "have lost or are subject to losing money and property." *Id.* However, they do not allege that either named Plaintiff has suffered any actual injury thus far.⁴

Plaintiffs subsequently filed the present action asserting five claims arising under federal and Maryland law: negligence (Count I); breach of implied contract (Count II); unjust enrichment (Count III); declaratory judgment pursuant to the Declaratory Judgment Act, 28 U.S. Code §§ 2201 (Count IV); and the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501, *et seq.* (Count V). On Defendants' motion, this Court entered a stay on April 21, 2016 (ECF No. 20) pending the resolution of Defendants' Motion to Dismiss. This Court then conducted a hearing on May 19, 2016 on the present Motion.

STANDARD OF REVIEW

Defendants move to dismiss the present Complaint pursuant to Rule 12(b)(1) and Rule 12(b)(6) of the Federal Rules of Civil Procedure. As this Opinion addresses only Defendants' jurisdictional objections, Rule 12(b)(1) is the appropriate standard of review. A motion to dismiss under Rule 12(b)(1) of the Federal Rules of Civil Procedure for lack of subject matter jurisdiction challenges a court's authority to hear the matter brought by a complaint. *See Davis v. Thompson*, 367 F. Supp. 2d 792, 799 (D. Md. 2005). This challenge

⁴ As will be discussed *supra*, Plaintiffs' counsel asserted at the May 19 hearing that Chambliss had expended resources to engage a credit monitoring service to mitigate the risk of identity theft allegedly created by the data breach. Apart from this mitigation expense, however, Plaintiffs do not allege any actual monetary injury.

under Rule 12(b)(1) may proceed either as a facial challenge, asserting that the allegations in the complaint are insufficient to establish subject matter jurisdiction, or a factual challenge, asserting “that the jurisdictional allegations of the complaint [are] not true.” *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009) (citation omitted). With respect to a facial challenge, a court will grant a motion to dismiss for lack of subject matter jurisdiction “where a claim fails to allege facts upon which the court may base jurisdiction.” *Davis*, 367 F. Supp. 2d at 799.

Where the challenge is factual, “the district court is entitled to decide disputed issues of fact with respect to subject matter jurisdiction.” *Kerns*, 585 F.3d at 192. “[T]he court may look beyond the pleadings and ‘the jurisdictional allegations of the complaint and view whatever evidence has been submitted on the issue to determine whether in fact subject matter jurisdiction exists.’” *Khoury v. Meserve*, 268 F. Supp. 2d 600, 606 (D. Md. 2003) (citation omitted). The court “may regard the pleadings as mere evidence on the issue and may consider evidence outside the pleadings without converting the proceeding to one for summary judgment.” *Velasco v. Gov’t of Indon.*, 370 F.3d 392, 398 (4th Cir. 2004); *see also Sharafeldin v. Md. Dep’t of Pub. Safety & Corr. Servs.*, 94 F. Supp. 2d 680, 684-85 (D. Md. 2000). A plaintiff carries the burden of establishing subject matter jurisdiction. *Lovern v. Edwards*, 190 F.3d 648, 654 (4th Cir. 1999).

ANALYSIS

In moving to dismiss the present Complaint pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure, Defendants argue that the Plaintiffs have failed to allege a

sufficient injury in fact to satisfy Article III of the Constitution.⁵ Plaintiffs thus lack standing, thereby depriving this Court of the requisite subject-matter jurisdiction to adjudicate their claims. Article III, Section 2 places certain restraints on the federal courts, including limiting the courts to the resolution of actual cases and controversies. U.S. Const. art. III, § 2. As the United States Court of Appeals for the Fourth Circuit has explained, “[a]mong ‘the several doctrines that have grown up to elaborate that requirement,’ the one ‘that requires a litigant to have ‘standing’ to invoke the power of a federal court is perhaps the most important.’” *Friends for Ferrell Parkway, LLC v. Stasko*, 282 F.3d 315, 319 (4th Cir. 2002) (quoting *Allen v. Wright*, 486 U.S. 737, 750 (1984)); accord *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 153 (4th Cir. 2000) (en banc).

To establish the “irreducible constitutional minimum of standing,” a plaintiff must satisfy the following criteria. First, that she suffered an “injury in fact,” which is an “invasion of a legally protected interest which is (a) concrete and particularized, . . . and (b) actual or imminent, not conjectural or hypothetical.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal citations and quotation marks omitted). Second, the injury must be “fairly traceable to the challenged action of the defendant.” *Friends for Ferrell Parkway*, 282 F.3d at 320 (citing *Friends of the Earth, Inc. v. Laidlaw Envil. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); *Lujan*, 504 U.S. at 560-61; *Allen*, 468 U.S. at 751). Third, it must be “likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Id.*

⁵ As noted *supra*, Defendants also move to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. Plaintiffs have failed to allege the requisite injury in fact for Article III standing, thus this Court need not consider Defendants’ Rule 12(b)(6) arguments.

The plaintiff bears the burden of establishing standing, as he “is the party seeking to invoke federal jurisdiction.” *Friends for Ferrell Parkway*, 282 F.3d at 320 (citing *Lujan*, 504 U.S. at 561). Where the lawsuit is a putative class action, any named plaintiffs must allege that they personally have been injured. *Warth v. Seldin*, 422 U.S. 490, 502 (1975). They may not rely on injuries suffered by unknown class members to confer standing. *Id.*; see also *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974) (“[I]f none of the named plaintiffs purporting to represent a class establishes the requisite case or controversy with the defendants, none may seek relief on behalf of himself or any member of the class.”).

At issue in the present case is the first element of standing—whether Plaintiffs have suffered an “injury in fact” that is concrete, particularized, and actual or imminent. *Gaston Copper Recycling Corp.*, 204 F.3d at 154 (citing *Lujan*, 504 U.S. at 560-61). When the plaintiff alleges an injury based on future harm, “the threatened injury must be *certainly impending* to constitute injury in fact.” *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (2013) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (emphasis in original)). Mere “allegations of possible future injury are not sufficient.” *Id.* (emphasis in original). In other words, there must be a “substantial risk” that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper*, 133 S. Ct. at 1147, 1150 n.5). The requirement that the harm be certainly impending “ensure[s] that the alleged injury is not too speculative for Article III purposes.” *Lujan*, 504 U.S. at 564 n.2. Where the alleged injury requires a lengthy chain of assumptions, including “guesswork as to how independent decisionmakers will exercise their judgment,” the injury is too speculative to be “certainly impending.” *Clapper*, 133 S. Ct. at 1150. See also *Roy v. Ward Mfg., LLC*, Civ. A. No RDB-13-3878, 2014 WL

4215614, at *3 (D. Md. Aug. 22, 2014) (noting that standing is absent where the plaintiffs must rely on “an extensive chain of unlikely events before establishing any potential injury.”).

In this case, Plaintiffs assert four forms of injury stemming from the CareFirst data breach: (1) an increased risk of identity theft; (2) mitigation costs incurred; (3) benefit of the bargain loss; and (4) decreased value of their personal information. Defendants contend that none of the alleged injuries is a sufficient injury in fact that could confer Article III standing. Each injury will be addressed in turn.

1. Increased Risk of Future Harm

Plaintiffs allege that, due to Defendants’ failure to secure adequately their personal information, they face an increased risk that unknown hackers will use that information for fraudulent charges and other forms of identity theft. As neither named Plaintiff has yet to suffer any misuse of his or her data, however, CareFirst argues that this increased risk of future harm is far too speculative to constitute a cognizable injury in fact.

Although no courts in this circuit have addressed the standing requirements in the context of data breach litigation, most courts to consider the issue “have agreed that the mere loss of data—without any evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.” *In re Science Applications Int’l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19 (D.D.C. 2014); *accord In re Zappos.com, Inc.*, No. 3:12-cv-325, 2015 WL 3466943, at *8 (D. Nev. June 1, 2015); *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. 13-7418, 2-15 WL 1472483, at *6 (D.N.J. Mar. 31, 2015); *Green v. eBay, Inc.*, No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015); *Key v. DSW*,

Inc., 454 F. Supp. 2d 684, 689 (S.D. Ohio 2006). Indeed, “since *Clapper* . . . courts have been even more emphatic in rejecting ‘increased risk’ as a theory of standing in data-breach cases.” *Science Applications*, 45 F. Supp. 3d at 28; *accord Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014); *In re SuperValu, Inc.*, No. 14-MD-2586 ADM/TNL, slip op., 2016 WL 81792, at *4 (D. Minn. Jan. 7, 2016).

Key to the speculative nature of this theory of harm is its dependence on a chain of assumptions that must occur before the harm materializes. As the United States District Court for the District of Minnesota explained, the “numerous variables . . . include[e] whether the hacker: (1) read, copied, and understood [Plaintiffs’] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs’] names.” *In re SuperValu*, 2016 WL 81792, at *5 (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011)). This reliance on the actions of an unknown independent third party creates a theory of injury that only amounts to an “objectively reasonable likelihood of harm.” *Science Applications*, 45 F. Supp. 3d at 25-26. Under *Clapper*, however, “an ‘objectively reasonable likelihood’ of harm is not enough to create standing, even if it is enough to engender some anxiety.” *Id.* at 26 (citing *Clapper*, 133 S. Ct. at 1147-48).

In this case, Plaintiffs do not allege that their data has been misused in any way thus far. The breach compromised only Plaintiffs’ names, birthdates, email addresses, and subscriber identification numbers, and not their social security numbers, credit card information, or any other similarly sensitive data that could heighten the risk of harm. Plaintiffs contend that their personal information has value, but have not alleged how a

hacker would use the particular information stolen to harm the Plaintiffs. Their theory of harm relies solely on the actions of an unknown independent third party. It is thus not clear “*whether* future harm from a data security breach will materialize,” but also uncertain “*when* such harm will occur.” *In re SuperValu*, 2016 WL 81792, at *5. The data breaches allegedly occurred in June 2014 and May 2015, yet to this day, neither Plaintiff has suffered any fraudulent charges or other evidence of misuse. The imminence of the asserted harm thus becomes ever less likely as the breaches fade further into the past. *In re Zappos*, 2015 WL 3466943, at *8; *In re SuperValu*, 2016 WL 81792, at *5.

Plaintiffs’ efforts to establish the imminence of their theory of harm are unpersuasive. Indeed, the cases upon which they rely do not contradict this Court’s conclusion, but rather demonstrate the factual allegations necessary to establish standing in data breach litigation. Specifically, those cases either concerned information more easily used in fraudulent transactions or relied on factual allegations that the hackers had already misused the stolen data such that the risk of future harm was certainly impending. *See Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692-94 (7th Cir. 2015) (over 9,200 customers had experienced fraudulent charges, thus “there was no need to speculate” as to whether the harm was imminent); *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (since stolen data had already surfaced on the internet, the risk of harm was “immediate and very real”); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (harm not speculative, as the plaintiffs had alleged “unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees”); *In re Sony Gaming Networks and Customer Data Breach Sec. Litig.*, 996 F. Supp. 2d 942, 962

(S.D. Cal. 2014) (alleged data stolen included credit and debit card numbers, expiration dates, and other information necessary to use the cards).

Plaintiffs' allegations stand in stark contrast to those cases finding standing. Plaintiffs do not cite to a single instance of data misuse even though a significant amount of time has passed since the data breaches. They even acknowledged at the May 19 hearing that any amended complaint would not include new allegations of misuse. Moreover, where credit card and social security numbers are stolen, the future harm is not speculative as “[w]hy else would hackers break into a store's database and steal consumers' private information?” *Remijas*, 794 F.3d at 694. In this case, it is not as readily apparent how a potential hacker would use the information stolen in this case to harm the Plaintiffs. Accordingly, Plaintiffs have failed to allege sufficient facts to show that the future harm from the CareFirst data breach is “certainly impending” or that there is “a substantial risk that the harm will occur.” *Clapper*, 133 S. Ct. at 1147, 1150 n.5.

2. Mitigation Costs

Plaintiffs next allege that they have suffered harm in the form of mitigation costs, specifically expenses incurred from obtaining credit-monitoring services. Only Chambliss, and not Adamson, has purchased such services. Yet, a plaintiff “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper*, 133 S. Ct. at 1151. As the Supreme Court explained, the opposite conclusion would allow “an enterprising plaintiff . . . to secure a lower standard for Article III standing simply by making an expenditure based on a

nonparanoid fear.” *Id.* In other words, the harm must thus be “certainly impending” before mitigation expenses may be considered as further proof of a cognizable injury.

In the context of data breach litigation, courts have consistently held that a plaintiff may not use mitigation costs alone to establish a cognizable injury in fact. *See, e.g., In re Adobe*, 66 F. Supp. 3d at 1216-17. Rather, the plaintiff must first show that the harm is “certainly impending” before costs to mitigate against that risk will also be an injury in fact. *Id.; see also Science Applications*, 45 F. Supp. 3d at 26; *In re Zappos*, 2015 WL 3466943, at *10; *Remijas*, 794 F.3d at 694; *Lewert v. P.F. Chang's China Bistro*, --- F.3d ----, 2016 WL 1459226, at * 3 (7th Cir. 2016). In this case, the future harm to be mitigated by Chambliss’s purchase of credit-monitoring services is not “certainly impending.” As such, her mitigation expenses do not constitute an injury in fact for purposes of Article III standing.

3. Benefit of the Bargain Loss

Third, Plaintiffs allege that they were harmed by the lost benefit of their bargain with CareFirst.⁶ As the *In re SuperValu* Court explained, however, “[t]his theory is consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach.” *In re SuperValu*, 2016 WL 81792, at *8. For example, in *In re Zappos*, 2015 WL 3466943, at *11 n.5, the United States District Court for the District of Nevada rejected the plaintiffs’ benefit-of-the-bargain theory because the plaintiffs failed to explain how the data breach affected the value of the goods purchased. Even further, the *In re Zappos* plaintiffs alleged no facts indicating that the

⁶ Plaintiffs do not allege this loss in their Complaint, but rather stated during the May 19 hearing that any amended complaint would include such allegations. In the interests of judicial economy and efficiency, this Court will address this alleged injury.

prices they paid incorporated some form of protection premium that the plaintiffs knew would be used to secure their data. *Id.*; *see also Remijas*, 794 F.3d at 694-95 (stating that benefit-of-the-bargain injuries or “would not have shopped” damages are “dubious”); *P.F. Chang’s*, 2016 WL 1459226, at *4 (explaining that such arguments have “been adopted by courts only where the product itself was defective or dangerous and consumers claim they would not have bought it (or paid a premium for it) had they known of the defect.”).

Here, Plaintiffs make no allegations that the data breach diminished the value of the health insurance they purchased from CareFirst. Even further, they offer no factual allegations indicating that the prices they paid for health insurance included a sum to be used for data security, and that both parties understood that the sum would be used for that purpose. Indeed, when pressed at the May 19 hearing, Plaintiffs could not even quantify this alleged loss. Accordingly, Plaintiffs have not alleged any benefit-of-the-bargain loss that could constitute a cognizable injury in fact.

4. Decreased Value of Personal Information

Finally, Plaintiffs argue that their personal information has an intrinsic value that was diminished as a result of the CareFirst data breach. This Court need not decide whether such personal information has a monetary value, as Plaintiffs have not alleged that they have attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information. *In re SuperValu*, 2016 WL 81792, at *7; *see also Science Applications*, 45 F. Supp. 3d at 30 (finding no injury in fact where the plaintiffs had not alleged that they the data breach compelled them to sell their data at a below-value price); *In re Zappos*, 2015 WL 3466943, at *3 (finding the same); *Green*, 2015 WL 2066531, at

*5 n.59 ("Even if the Court were to find that personal information has an inherent value . . . Plaintiff has failed to allege facts indicating how the value of his personal information has decreased as a result of the Data Breach."). Plaintiffs have thus failed to allege an injury in fact based on any diminution of the value of their personal information.

CONCLUSION

For the reasons stated above, Defendants' Motion to Dismiss (ECF No. 11) is GRANTED. In sum, Plaintiffs have failed to allege facts sufficient to establish standing under Article III of the Constitution. Accordingly, this Court does not have subject matter jurisdiction to adjudicate their claims. All claims are thus DISMISSED.

A separate Order follows.

Dated: May 29, 2016

Richard D. Bennett
Richard D. Bennett
United States District Judge